

The University of Chicago

IDEALS IN CUBIC AND CERTAIN QUARTIC FIELDS

A DISSERTATION SUBMITTED TO THE
FACULTY OF THE DIVISION OF THE
PHYSICAL SCIENCES IN CANDIDACY
FOR THE DEGREE OF DOCTOR OF
PHILOSOPHY

DEPARTMENT OF MATHEMATICS

1937

By
HARRIET REES

Private Edition, Distributed by
THE UNIVERSITY OF CHICAGO LIBRARIES
CHICAGO, ILLINOIS
1937

The University of Chicago

IDEALS IN CUBIC AND CERTAIN QUARTIC FIELDS

A DISSERTATION SUBMITTED TO THE
FACULTY OF THE DIVISION OF THE
PHYSICAL SCIENCES IN CANDIDACY
FOR THE DEGREE OF DOCTOR OF
PHILOSOPHY

DEPARTMENT OF MATHEMATICS

1937

By
HARRIET REES

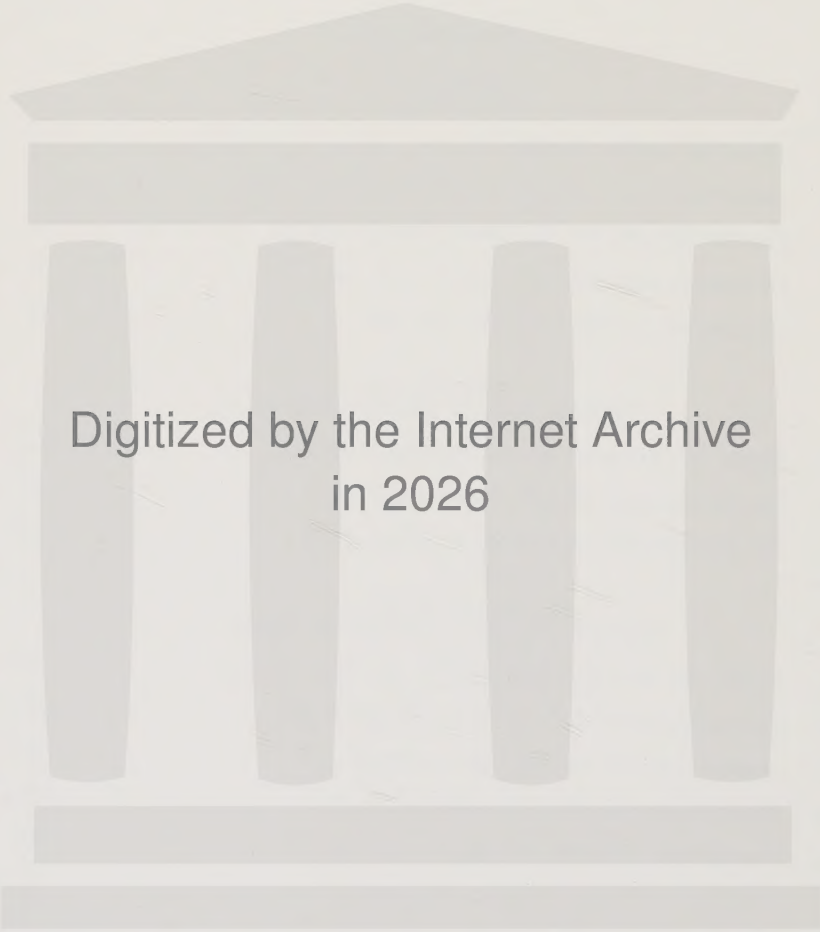
Private Edition, Distributed by
THE UNIVERSITY OF CHICAGO LIBRARIES
CHICAGO, ILLINOIS

1937



TABLE OF CONTENTS

	INTRODUCTION	Page 1
	CHAPTER I CUBIC FIELDS	
Section		
1.	Bases of cubic fields	3
2.	Criterion for factorization of (p) in $R(\theta)$	5
3.	Factorization of (p) when $e \not\equiv 0 \pmod{p}$	7
4.	Factorization of (p) when $e \equiv 0 \pmod{p}$	9
5.	The prime factors of (2) and (3)	11
	CHAPTER II CERTAIN CYCLIC QUARTIC FIELDS	
6.	Bases of certain cyclic quartic fields	16
7.	Factorization of (p) when $(w p) = -1$	18
8.	Factorization of (p) when $(w p) \neq -1$	19
	CHAPTER III CERTAIN NON-CYCLIC QUARTIC FIELDS	
9.	Bases of certain non-cyclic quartic fields	24
10.	Factorization of (p) when $(4r p) = -1$	25
11.	Factorization of (p) when $(4r p) = 1$	28
12.	Factorization of (p) when $(r p) = 0$	30
13.	The prime factors of (2)	31



Digitized by the Internet Archive
in 2026

https://archive.org/details/IA41548407_0087

IDEALS IN CUBIC AND CERTAIN QUARTIC FIELDS

INTRODUCTION

Let R be the field of all rational numbers. Consider the field $R(\sqrt[3]{J})$, where $\sqrt[3]{J}$ is a root of a rational equation irreducible in R . A system M of integral numbers of $R(\sqrt[3]{J})$ is called an ideal if, for every α and β of M , $\lambda\alpha + \mu\beta$ is in M for arbitrary integral coefficients λ, μ of $R(\sqrt[3]{J})$. An ideal, different from the unit ideal, is said to be prime if it has no divisors except itself and the unit ideal. Every ideal contains a rational integer, for, if α is in M , the rational integer $N(\alpha) = \text{norm } \alpha$ is in M . If M is prime, it divides a prime factor of $N(\alpha)$ and no other prime, for M is not the unit ideal. Thus the prime ideals of $R(\sqrt[3]{J})$ are exactly the prime ideal factors of the rational primes.

By a basis of M is meant a set of n numbers $\alpha_1, \dots, \alpha_n$ such that $\alpha = a_1\alpha_1 + \dots + a_n\alpha_n$ ranges over all the integers of M precisely once as $a_1, \dots, a_n$ range over all the rational integers. Let small Roman letters represent rational integers and Greek letters algebraic integers. If a basis of the integers of $R(\sqrt[3]{J})$ over the rational integers is given by $1, \omega_2, \dots, \omega_n$, M has a basis $r, s + t\omega_2, \dots, x + y\omega_2 + \dots + z\omega_n$. The integer r is the g.c.d. of all rational integers of M , t is the g.c.d. of the coefficients of ω_2 in integers of M of the form $b + c\omega_2, \dots$, and z is the g.c.d. of the coefficients of ω_n in integers of M of the form $d + e\omega_2 + \dots + f\omega_n$. The necessary

and sufficient conditions that such a set of elements be basal elements of the ideal which they generate are the closure conditions that arise by multiplying each element of the set by each basal element $\omega_2, \dots, \omega_n$ of the field and expressing each such product linearly, with rational integral coefficients, in terms of the elements of the set. The problem of this paper is to determine explicit bases for the prime ideals of all cubic and certain quartic fields.

CHAPTER I

CUBIC FIELDS

In this chapter, the ideals of cubic fields are considered. In the quadratic and quartic cases that have been investigated, the criterion for factorization of a rational prime p into prime ideal factors has been expressed in terms of Kronecker symbols $(x|p)$, where x is a factor of the discriminant of the field. In the case of a cubic field, the criterion involves the factorization modulo p of a cubic equation which generates the field and cannot always be expressed in terms of a Kronecker symbol. With this exception, there is no noteworthy distinction between the cubic and quartic cases.

1. Bases of cubic fields. It has been proved by A. A. Albert¹ that every cubic field F has a generation $F = R(\theta)$, $\theta^3 + a\theta + b = 0$, where a has no prime factor p such that p^2 divides b . Moreover, a and b satisfy one of the mutually exclusive conditions

- | | | |
|-----|------------------------------|------------------------|
| (1) | $b \equiv 1 \pmod{2},$ | |
| (2) | $b \equiv 2 \pmod{4},$ | $a \equiv 0 \pmod{2},$ |
| (3) | $b \equiv 0 \pmod{4},$ | $a \equiv 1 \pmod{4},$ |
| (4) | $b \equiv 2 \pmod{4},$ | $a \equiv 3 \pmod{4},$ |
| (5) | $b \equiv (a + 1) \pmod{8},$ | $a \equiv 3 \pmod{4}.$ |

In addition, a and b may be taken to satisfy one of

¹A. A. Albert, Normalized integral bases of algebraic number fields, Annals of Mathematics, vol. 38 (1937).

- (6) $a \not\equiv 0 \pmod{3}$,
 (7) $a \equiv 6 \pmod{9}$, b exactly divisible by 3,
 (8) $a \equiv 0 \pmod{9}$, $b \equiv 2, 4, 5, 7 \pmod{9}$,
 (9) $a \equiv 6 \pmod{9}$, $b \equiv 1, 8 \pmod{9}$,
 (10) $a \equiv 6 \pmod{9}$, $b \equiv 4, 5 \pmod{9}$,
 (11) $a \equiv 0 \pmod{9}$, b exactly divisible by 3,
 (12) $a \equiv 6 \pmod{9}$, $b \equiv 0 \pmod{9}$,
 (13) $a \equiv 0 \pmod{9}$, $b \equiv 1, 8 \pmod{9}$.

Write $a = ka_0$, $b = kb_0$ where a_0 and b_0 have no common prime factors except 2 and 3, and $(k, 6) = 1$. By the symbol $(k, 6)$ is meant the g.c.d. of k and 6. Let $4a_0^3k + 27b_0^2 = 2^{2u}3^{2v}q^2d_0$ with $(q, 6) = 1$ and d_0 a product of distinct primes. The integers a , b may be so chosen that q is prime to kd_0 . A basis² of $R(\theta)$ over the rational integers is given by

$$1, \theta, \omega = (a + c^2 + c\theta + \theta^2)/e,$$

where $e = 2^f3^hq$. In cases (1), ..., (4), $f = 0$, while in (5), $f = 1$; in cases (6), ..., (11), $h = 0$, but in (12) and (13) $h = 1$. All conditions on c are satisfied by taking

$$c \equiv 1 \pmod{2}, \quad c + b \equiv 0 \pmod{3}, \quad 2ac + 3b \equiv 0 \pmod{q}.$$

Since the discriminant of $f(x)$ is given by

$$d(\theta) = -4a^3 - 27b^2 = -2^{2u}3^{2v}k^2q^2d_0,$$

the discriminant d of $R(\theta)$ is given by

$$d = -2^{2(u-f)}3^{2(v-h)}k^2d_0.$$

²Ibid.

2. Criterion for factorization of (p) in $R(\theta)$. Let p represent a rational prime. If an ideal M different from the unit ideal is a divisor of the principal ideal (p) generated by p and is different from (p) , M must have the basal elements p , $r + s\theta$, $t + u\theta + v\omega$, hence $\text{norm } M = N(M) = psv$. If $MQ = (p)$, $N(M)N(Q) = N(p) = p^3$, hence $sv \neq p^2$ must divide p^2 . If $s = p$, $-p\theta + r + p\theta$ is in M , hence $r \equiv 0 \pmod{p}$. Since any three elements of M obtainable from a set of basal elements by a transformation of determinant ± 1 also form a basis of M , r may be taken equal to zero. Similarly, if $s = 1$ we may take $u = 0$. If also $v = p$, $t + p\omega - p\omega$ is in M , hence $t = 0$.

LEMMA 1. Every ideal divisor $\neq (1)$ or (p) in $R(\theta)$ of (p) is one of

$$I = [p, x + \theta, y + \omega],$$

$$J = [p, z + \theta, p\omega], \quad K = [p, p\theta, s + t\theta + \omega].$$

The bracket notation indicates that the ideal is expressed in terms of its basal elements.

We compute the closure conditions for I . Let $p\theta = a_1p + a_2(x + \theta) + a_3(y + \omega)$ and $p\omega = a_4p + a_5(x + \theta) + a_6(y + \omega)$, the a_i rational integers. Since 1 , θ , and ω are linearly independent over R , we may equate coefficients of like elements in each equation. In these cases, no conditions on x and y are obtained. Let $\theta(x + \theta) = b_1p + b_2(x + \theta) + b_3(y + \omega)$. Using

$$\theta^2 = -a - c^2 - c\theta + e\omega,$$

the above equation becomes

$$-a - c^2 + (x - c)\theta + e\omega = b_1p + b_2(x + \theta) + b_3(y + \omega).$$

Therefore $e = b_3$, $x - c = b_2$, $-a - c^2 = b_1p + b_2x + b_3y$ and

$$(14) \quad x^2 - cx + ey + a + c^2 \equiv 0 \pmod{p}.$$

Let $\omega(x + \theta) = b_4p + b_5(x + \theta) + b_6(y + \omega)$. Using

$$\theta\omega = -m\epsilon + c\omega, \quad m = (c^3 + ac + b)/\epsilon^2,$$

this equation becomes

$$-m\epsilon + (x + c)\omega = b_4p + b_5(x + \theta) + b_6(y + \omega).$$

Thus we find

$$(15) \quad y(x + c) + \epsilon m \equiv 0 \pmod{p}.$$

Let $\omega(y + \omega) = c_1p + c_2(x + \theta) + c_3(y + \omega)$. Using

$$\omega^2 = -2mc - m\theta + n\omega, \quad n = (3c^2 + a)/\epsilon,$$

this equation becomes

$$-2mc - m\theta + (y + n)\omega = c_1p + c_2(x + \theta) + c_3(y + \omega),$$

hence

$$(16) \quad y^2 + ny - mx + 2cm \equiv 0 \pmod{p}.$$

From $\theta(y + \omega) = c_4p + c_5(x + \theta) + c_6(y + \omega)$ no new condition is obtained.

In a similar manner it can be shown that the closure conditions for J are given by

$$(17) \quad z^2 - cz + a + c^2 \equiv 0 \pmod{p},$$

$$(18) \quad z + c \equiv 0 \pmod{p},$$

$$(19) \quad e \equiv 0 \pmod{p},$$

and the closure conditions for K by

$$(20) \quad s(n + s + ct) + m(2c + \epsilon t) \equiv 0 \pmod{p},$$

$$(21) \quad s(c + \epsilon t) + (a + c^2)t + \epsilon m \equiv 0 \pmod{p},$$

$$(22) \quad t(n + s + ct) + m \equiv 0 \pmod{p},$$

$$(23) \quad \epsilon t^2 + 2ct - s \equiv 0 \pmod{p}.$$

If the ideal (p) is not itself prime, it must have a factor I of norm p . Since $x + \theta$ is in I , $N(x + \theta)$ is in I , hence

$$(24) \quad -N(x + \theta) = f(-x) \equiv 0 \pmod{p}.$$

Conversely, suppose that x' is a solution of (24) and consider $M = (p, x' + \theta)$. If $M = (p)$, $x' + \theta = p(d_1 + d_2\theta + d_3\omega)$, hence d_2 is not an integer. Further, any α in M may be written $\alpha = \beta p + \gamma(x' + \theta)$, β and γ in $R(\theta)$. Since $N(x' + \theta) \equiv 0 \pmod{p}$, $N(\alpha) \equiv 0 \pmod{p}$ for every α of M . Thus $M \neq (1)$ or (p) and divides (p) , hence (p) is not prime.

THEOREM 1. A necessary and sufficient condition that the ideal generated by a rational prime p factor in $R(\theta)$ is that there exist a solution x' of (24). Then $M = (p, x' + \theta)$ is a factor of (p) .

3. Factorization of (p) when $e \not\equiv 0 \pmod{p}$. Suppose M is a factor of (p) . If $M = K$, then $x' + \theta = a_1p + a_2p\theta + a_3(s + t\theta + \omega)$ and a_2 is not an integer. If $M = J$, (19) demands $e \equiv 0 \pmod{p}$. Thus $e \not\equiv 0 \pmod{p}$ implies that $M = I$. From $x' + \theta = a_4p + a_5(x + \theta) + a_6(y + \omega)$ we have $x' \equiv x \pmod{p}$. Moreover, y is uniquely determined by (14).

Since J cannot be a divisor of (p) , K must be, and

$$(25) \quad (p) = [p, x + \theta, y + \omega][p, p\theta, s + t\theta + \omega].$$

Therefore

$$\begin{aligned} (x + \theta)(s + t\theta + \omega) &= -em - (a + c^2)t + xs + (s - ct + xt)\theta \\ &\quad + (c + et + x)\omega \\ &= p(b_1 + b_2\theta + b_3\omega), \end{aligned}$$

hence $c + et + x = pb_1$, $s - ct + xt = pb_2$ and s and t are uniquely determined by

$$(26) \quad et \equiv -x - c \pmod{p},$$

$$(27) \quad s \equiv t(c - x) \pmod{p}.$$

If $f(x) \equiv (x + x_1)(x + x_2)(x + x_3) \pmod{p}$ is a factorization of $f(x)$ modulo p , it can be shown³ that $(p) = (p, x_1 + \theta)(p, x_2 + \theta)(p, x_3 + \theta)$. Then, by the previous discussion,

$$(28) \quad (p) = [p, x_1 + \theta, y_1 + \omega][p, x_2 + \theta, y_2 + \omega][p, x_3 + \theta, y_3 + \omega],$$

where the y_i are determined by congruences corresponding to (14). If (24) has a single solution x , then K must be prime or else divisible by I . Suppose that the latter holds. Then

$$s + t\theta + \omega = a_1p + a_2(x + \theta) + a_3(y + \omega)$$

and

$$(29) \quad s - tx - y \equiv 0 \equiv e(x - tx - y) \pmod{p}.$$

Using (26), (27), and (14), (29) becomes

$$(30) \quad 3x^2 + a \equiv 0 \pmod{p}.$$

But x can be a solution of (24) and (30) only if it is a double solution of (24), contrary to the assumption. Therefore K is prime.

THEOREM 2. Suppose that $e \not\equiv 0 \pmod{p}$ and that (p) factors in $R(\theta)$. When x_1, x_2 , and x_3 are solutions of (24), the prime factors of (p) in $R(\theta)$ are given by (28), where

$$ey_1 \equiv -x_1^2 + cx_1 - a - c^2 \pmod{p} \quad (i = 1, 2, 3),$$

but when x is the only solution of (24), the prime factors of (p) are given by (25) with y determined by (14), t by (26), and s by (27).

³J. Sommer, Vorlesungen über Zahlentheorie, 1907, pp. 278-283.

4. Factorization of (p) when $e \equiv 0 \pmod{p}$. Since $m = (c^3 + ac + b)/e^2$ is an integer of $R(\theta)$, $-c$ is a solution of (24) and (p) always factors. Hence, by the lemma, $(p) = IK$ or I_1J , where

$$I_1 = [p, x_1 + \theta, y_1 + \omega],$$

If $(p) = IK$

$$\begin{aligned} (x + \theta)(s + t\theta + \omega) &= -em - (a + c^2)t + xs + (s - ct + xt)\theta \\ &\quad + (c + et + x)\omega \\ &= p(a_1 + a_2\theta + a_3\omega), \\ (y + \omega)(s + t\theta + \omega) &= -2mc - emt + sy + (yt - m)\theta \\ &\quad + (n + s + ct + y)\omega \\ &= p(a_4 + a_5\theta + a_6\omega), \end{aligned}$$

hence $c + et + x \equiv 0 \pmod{p}$, $s - ct + xt \equiv 0 \pmod{p}$,
 $n + s + ct + y \equiv 0 \pmod{p}$, $yt - m \equiv 0 \pmod{p}$. Combining these congruences, we find

$$\begin{aligned} (31) \quad x + c &\equiv 0 \pmod{p}, \\ (32) \quad s - 2ct &\equiv 0 \pmod{p}, \\ (33) \quad y + 3ct + n &\equiv 0 \pmod{p}, \\ (34) \quad 3ct^2 + nt + m &\equiv 0 \pmod{p}. \end{aligned}$$

If $(p) = I_1J$,

$$\begin{aligned} (z + \theta)(y_1 + \omega) &= -em + zy_1 + y_1\theta + (c + z)\omega \\ &= p(b_1 + b_2\theta + b_3\omega), \\ (z + \theta)(x_1 + \theta) &= -a - c^2 + zx_1 + (z + x_1 - c)\theta + e\omega \\ &= p(b_4 + b_5\theta + b_6\omega). \end{aligned}$$

As above, it is seen that

$$(35) \quad z \equiv -c \pmod{p}, \quad y_1 \equiv 0 \pmod{p}, \quad x_1 \equiv 2c \pmod{p}.$$

If (34) has a solution t and if s is determined by (32), the closure conditions for K are satisfied and $K \neq (1)$ or (p) divides (p) . Similarly, J is a factor of (p) .

We consider first the prime factors of (p) when $q \equiv 0 \pmod{p}$. Since $(p, 6abc) = 1$, (34) has a solution if and only if

$$48a^4c(3ct^2 + nt + m) = (12a^2ct + 2na^2)^2 - (2a^2)^2(n^2 - 12cm) \\ \equiv 0 \pmod{p}$$

has a solution. But

$$(12a^2b)^2(n^2 - 12cm) = 4a^2(2ac + 3b)^2(4a^4 - 12a^2bc - 27b^2c^2)/e^2 \\ + 4a^2c(2ac + 3b)(18bc + 4a^2 - 12bc)d \\ + (2ac)^2dd(\theta) - 96a^3bc^3d.$$

Let $2ac + 3b = kq$. Then

$$(12a^2b)^2(n^2 - 12cm) = k^2q^2(16a^6 + 72a^3b^2 - 243b^4 + qr_1)/e^2 \\ + 324b^4d + qr_2 \\ = k^2q^2\{d(\theta)[36b^2 + d(\theta)] + qr_1\}/e^2 \\ + 324b^4d + qr_2 \\ = k^2q^2d[36b^2 + d(\theta)] + k^2q^3r_1/e^2 \\ + 324b^4d + qr_2.$$

Thus

$$(12a^2b)^2(n^2 - 12cm) \equiv 2^23^4b^4d \pmod{p}$$

or

$$(2a^2)^2(n^2 - 12cm) \equiv (3b)^2d \pmod{p}.$$

Since $(q, d) = 1$, we conclude that (34) has a solution if and only if $(d|p) = 1$.

If $(d|p) = -1$, K cannot exist, hence $(p) = I_1J$. If $(d|p) = 1$, (34) has two solutions t_1 and t_2 , hence we have three valid factorizations for (p) :

$$\begin{aligned}
 (p) &= [p, -c + \theta, -3ct_1 - n + \omega][p, p\theta, 2ct_1 + t_1\theta + \omega], \\
 &= [p, -c + \theta, -3ct_2 - n + \omega][p, p\theta, 2ct_2 + t_2\theta + \omega], \\
 &= [p, 2c + \theta, \omega][p, -c + \theta, p\omega].
 \end{aligned}$$

But $p, -c + \theta, p\omega$ are in $I_2 = [p, -c + \theta, -3ct_1 - n + \omega]$, hence $[p, -c + \theta, p\omega]$ has a factor I_2 . It is a well known theorem⁴ that those primes and only those primes which divide the discriminant of an algebraic field F over R are divisible by the square of a prime ideal of F . Hence (p) is a product of three distinct prime ideals

$$(36) \quad (p) = [p, -c+\theta, -3ct_1-n+\omega][p, -c+\theta, -3ct_2-n+\omega][p, 2c+\theta, \omega].$$

THEOREM 3. Let $q \equiv 0 \pmod{p}$. If $(d|p) = -1$, the prime factors of (p) in $R(\theta)$ are given by

$$(p) = [p, 2c + \theta, \omega][p, -c + \theta, p\omega],$$

but if $(d|p) = 1$, the required factorization is given by (36) with t_1 and t_2 solutions of (34).

It is of interest to determine the factors of (2) and (3) when $e \not\equiv 0 \pmod{2, 3}$ as well as when $e \equiv 0 \pmod{2, 3}$. This is done in the following section.

5. The prime factors of (2) and (3). First consider the ideal (2). In cases (1), ..., (4), e is odd, hence we apply Theorems 1 and 2. In case (1), (24) becomes

$$x(a + 1) + 1 \equiv 0 \pmod{2},$$

hence a odd implies that (2) is prime, and a even implies that x odd is the only solution of (24). Then y is odd, t even, and s even.

⁴K. Hensel, Untersuchung der Fundamentalgleichung einer Gattung für reelle Primzahl als Modul und Bestimmung der Teiler ihrer Diskriminante, Crelle's Journal, vol. 113 (1894), pp. 61-83.

In cases (2), (3), and (4), (24) becomes

$$x(a + 1) \equiv 0 \pmod{2},$$

hence (2) always factors. In case (2), x even is a triple solution of (24) and y is odd. In cases (3) and (4), x odd is a double solution, x even a single solution of (24), and y is even.

In case (5), e is even, hence the theory developed in Section 4 must be applied. Congruence (34) becomes

$$t(n + 1) + m \equiv 0 \pmod{2}.$$

Since $c^3 + ac + b \equiv c(a + 1) + (a + 1) \equiv 0 \pmod{8}$ and $3c^2 + a \equiv 2 \pmod{4}$, t even or odd satisfies this congruence and y is odd or even respectively. Thus

$$\begin{aligned} (2) &= [2, 1 + \theta, 1 + \omega][2, 2\theta, \omega] \\ &= [2, 1 + \theta, \omega][2, 2\theta, \theta + \omega] \\ &= [2, \theta, \omega][2, 1 + \theta, 2\omega] \end{aligned}$$

and therefore (2) has the three distinct factors $[2, 1 + \theta, 1 + \omega]$, $[2, 1 + \theta, \omega]$, $[2, \theta, \omega]$.

Next, consider the prime factors of (3). In cases (6), ..., (11) $e \not\equiv 0 \pmod{3}$, hence Theorems 1 and 2 apply.

Let $a \equiv e \equiv 1 \pmod{3}$. Then (24), (14), (26), and (27) become

$$\begin{aligned} x^3 + x - b &\equiv 0 \pmod{3}, \\ y + x^2 + bx + 1 + b^2 &\equiv 0 \pmod{3}, \\ t \equiv b - x &\pmod{3}, \quad s \equiv 2t(b + x) \pmod{3}. \end{aligned}$$

If $b \equiv 0 \pmod{3}$, $x \equiv 0 \pmod{3}$ is the only solution of (24); hence (25) is the desired factorization, $y + 1 \equiv t \equiv s \equiv 0 \pmod{3}$. Similarly if $b \equiv 1 \pmod{3}$, $x \equiv y + 1 \equiv t \equiv s + 2 \equiv 2 \pmod{3}$, and if $b \equiv 2 \pmod{3}$, $x \equiv y \equiv t \equiv s + 1 \equiv 1 \pmod{3}$.

Let $a \equiv e - 1 \equiv 1 \pmod{3}$. Then (24) and (27) are as above, and (14) and (26) become

$$2y + x^2 + bx + 1 + b^2 \equiv 0 \pmod{3},$$

$$2t - b + x \equiv 0 \pmod{3}.$$

If $b \equiv 0 \pmod{3}$, $x \equiv y + 2 \equiv t \equiv s \equiv 0 \pmod{3}$. If $b \equiv 1 \pmod{3}$, $x \equiv y \equiv t + 1 \equiv s + 2 \equiv 2 \pmod{3}$. Finally, if $b \equiv 2 \pmod{3}$, $x \equiv y - 1 \equiv t - 1 \equiv s + 1 \equiv 1 \pmod{3}$.

Let $a \equiv 2 \pmod{3}$. Then (24) becomes

$$x^3 + 2x - b \equiv 0 \pmod{3}.$$

If $b \not\equiv 0 \pmod{3}$, (3) is prime, but if $b \equiv 0 \pmod{3}$, $x \equiv 0, 1, 2 \pmod{3}$ satisfies (24). Then $y \equiv 1, 0, 0 \pmod{3}$ respectively if $e \equiv 1 \pmod{3}$ and $y \equiv 2, 0, 0 \pmod{3}$ respectively if $e \equiv 2 \pmod{3}$.

In cases (7), ..., (11), (24) becomes

$$x^3 - b \equiv 0 \pmod{3};$$

hence (3) is always the cube of a prime ideal. If $b \equiv 0 \pmod{3}$, $x \equiv y \equiv 0 \pmod{3}$; if $b \equiv 1 \pmod{3}$, $x \equiv y + 1 \equiv 1 \pmod{3}$; and if $b \equiv 2 \pmod{3}$, $x \equiv y + 2 \equiv 2 \pmod{3}$.

In cases (12) and (13), $e \equiv 0 \pmod{3}$. Congruence (34) becomes

$$nt + m \equiv 0 \pmod{3}.$$

Since $(3c^2 + a)/3 = c^2 + a_1 \equiv b^2 + a_1 \pmod{3}$, $n \equiv 2 \pmod{3}$ in case (12) and $n \equiv 1 \pmod{3}$ in case (13). Hence, in both cases, there are two factorizations,

$$\begin{aligned} (3) &= [3, b + \theta, 2n + \omega][3, 3\theta, bt + t\theta + \omega] \\ &= [3, b + \theta, \omega][3, b + \theta, 3\omega]. \end{aligned}$$

But $[3, b + \theta, 3\omega]$ is divisible by $[3, b + \theta, \omega]$, hence $(3) = [3, b + \theta, \omega]^2 [3, b + \theta, 2n + \omega]$.

We have thus proved

THEOREM 4. The prime factorization of (2) in $R(\theta)$ is given by

$b \equiv 1 \pmod{2}$	$a \equiv 1 \pmod{2}$	$(2) = [2, 2\theta, 2\omega]$
	$a \equiv 0 \pmod{2}$	$(2) = [2, 1+\theta, 1+\omega] [2, 2\theta, \omega]$
$b \equiv 2 \pmod{4}$	$a \equiv 0 \pmod{2}$	$(2) = [2, \theta, 1+\omega]^3$
$b \equiv 0 \pmod{4}$	$a \equiv 1 \pmod{4}$	$(2) = [2, 1+\theta, \omega]^2 [2, \theta, \omega]$
$b \equiv 2 \pmod{4}$	$a \equiv 3 \pmod{4}$	
$b \equiv a + 1 \pmod{8}$	$a \equiv 3 \pmod{4}$	$(2) = [2, 1+\theta, 1+\omega] [2, 1+\theta, \omega] [2, \theta, \omega]$

The prime factorization of (3) in $R(\theta)$ is given by

$a \equiv 1 \pmod{3}$	$b \equiv 0 \pmod{3}$	$e \equiv 1 \pmod{3}$	$(3) = [3, \theta, 2+\omega] [3, 3\theta, \omega]$
		$e \equiv 2 \pmod{3}$	$(3) = [3, \theta, 1+\omega] [3, 3\theta, \omega]$
	$b \equiv 1 \pmod{3}$	$e \equiv 1 \pmod{3}$	$(3) = [3, 2+\theta, 1+\omega] [3, 3\theta, 2\theta+\omega]$
		$e \equiv 2 \pmod{3}$	$(3) = [3, 2+\theta, 2+\omega] [3, 3\theta, \theta+\omega]$
	$b \equiv 2 \pmod{3}$	$e \equiv 1 \pmod{3}$	$(3) = [3, 1+\theta, 1+\omega] [3, 3\theta, \theta+\omega]$
		$e \equiv 2 \pmod{3}$	$(3) = [3, 1+\theta, 2+\omega] [3, 3\theta, 2\theta+\omega]$
$a \equiv 2 \pmod{3}$	$b \not\equiv 0 \pmod{3}$	$e \not\equiv 0 \pmod{3}$	$(3) = [3, 3\theta, 3\omega]$
	$b \equiv 0 \pmod{3}$	$e \equiv 1 \pmod{3}$	$(3) = [3, \theta, 1+\omega] [3, 1+\theta, \omega] [3, 2+\theta, \omega]$
		$e \equiv 2 \pmod{3}$	$(3) = [3, \theta, 2+\omega] [3, 1+\theta, \omega] [3, 2+\theta, \omega]$
$a \equiv 0 \pmod{9}$	$b \equiv 3b' \pmod{9}$ $b' \not\equiv 0 \pmod{3}$	$e \not\equiv 0 \pmod{3}$	$(3) = [3, \theta, \omega]^3$
$a \equiv 0 \pmod{9}$	$b \equiv \frac{4}{7} \pmod{9}$		$(3) = [3, 1+\theta, \omega]^3$
$a \equiv 6 \pmod{9}$	$b \equiv \frac{1}{4} \pmod{9}$		
$a \equiv 0 \pmod{9}$	$b \equiv \frac{2}{5} \pmod{9}$		$(3) = [3, 2+\theta, \omega]^3$
$a \equiv 6 \pmod{9}$	$b \equiv \frac{8}{6} \pmod{9}$		
$a \equiv 6 \pmod{9}$	$b \equiv 0 \pmod{9}$	$e \equiv 3e'$ $e' \not\equiv 0 \pmod{3}$	$(3) = [3, \theta, \omega]^2 [3, \theta, 1+\omega]$
$a \equiv 0 \pmod{9}$	$b \equiv 1 \pmod{9}$		$(3) = [3, 1+\theta, \omega]^2 [3, 1+\theta, 2+\omega]$
$a \equiv 0 \pmod{9}$	$b \equiv 8 \pmod{9}$		$(3) = [3, 2+\theta, \omega]^2 [3, 2+\theta, 2+\omega]$

CHAPTER II

CERTAIN CYCLIC QUARTIC FIELDS

The bases of all normal quartic fields have been determined by A. A. Albert in his paper, "The Integers of Normal Quartic Fields."⁵ This determination involves many sub-cases, both in the cyclic and non-cyclic cases. It has seemed inadvisable to consider all of these, and so the work is restricted to the study of an arbitrary sampling of normal fields, with consequent illustration of the types of possible factorizations. In this chapter we consider a type of cyclic field.

6. Bases of certain cyclic quartic fields. Every cyclic quartic field over R has a generator μ which satisfies an equation

$$f(y) \equiv y^4 + 2q(m^2 + n^2)y^2 + q^2n^2(m^2 + n^2) = 0,$$

whose group with respect to R is the cyclic group. In this equation q is a product of distinct primes, $m^2 + n^2$ is not a perfect square, and $(m, n) = 1$. The roots of $f(y) = 0$ are μ , $-\mu$,

$g(\mu) = \mu[\mu^2 + q(2m^2 + n^2)]/qmn$, and $-g(\mu)$. Consequently, if

$\mathfrak{Y} = \mathfrak{Y}(\mu)$, the conjugates to $\mathfrak{Y}$ are $\mathfrak{Y}' = \mathfrak{Y}[g(\mu)]$, $\mathfrak{Y}'' = \mathfrak{Y}(-\mu)$, and $\mathfrak{Y}''' = \mathfrak{Y}[-g(\mu)]$.

Let $m^2 + n^2 = v^2w$, w a product of distinct primes, and let $\omega^2 = w$. Then $R(\omega)$ is a quadratic subfield of the normal quartic field $R(\mu)$. Suppose that $(q, v) = r$, so that $q = q_1r$,

⁵A. A. Albert, The integers of normal quartic fields, *Annals of Mathematics*, vol. 31 (1930), pp. 381-418.

$v = v_2^2 v_1 r$, where v_1 is a product of distinct primes. Suppose further that $(q_1, w) = q_3$ and $(v_1, w) = v_5$ so that $q_1 = q_3 q_4$, $v_1 = v_5 v_6$, $w = v_5 q_3 w_1$. Let $v_2 r \zeta = \mu$ and denote the Euler ϕ -function for n by ϕ . Then if w is even, a basis of the integers of $R(\mu)$ is given by⁶

$$1, \omega, \Delta = \zeta(1 + v m^{\phi-1} \omega)/n, \quad \epsilon = \omega \zeta / v_5 q_3.$$

The following formulae are stated for convenience in computation:

$$\begin{aligned} \mu^2 &= vq(-vw + m\omega), & [g(\mu)]^2 &= -2qv^2w - \mu^2, \\ \zeta &= n\Delta - vv_5 q_3 m^{\phi-1} \epsilon, & \epsilon\omega &= w_1 n \Delta - d_1 \epsilon, \\ \Delta\omega &= d_1 \Delta + d_2 \epsilon, & \Delta^2 &= d_3 + d_4 \omega, \\ \epsilon\Delta &= e_1 + e_2 \omega, & \epsilon^2 &= e_3 + e_4 \omega, \\ \Delta' &= d_5 \Delta + d_6 \epsilon, & \epsilon' &= e_5 \Delta + e_6 \epsilon, \\ \Delta'' &= -\Delta, & 1 &= d_5 e_6 - d_6 e_5, \\ \Delta''' &= -\Delta', & \omega' &= -\omega'' = \omega''' = -\omega \\ D &= (16q_4 v_6)^2 w^3, & \epsilon'' &= -\epsilon, \quad \epsilon''' = -\epsilon', \end{aligned}$$

where

$$\begin{aligned} d_1 &= vwm^{\phi-1}, & d_2 &= v_5 q_3 (1 - wv^2 m^{2\phi-2})/n, \\ d_3 &= -vv_1 q_1 w [(m^{\phi} - 1)^2/n^2 + m^{2\phi-2}], \\ d_4 &= v_1 q_1 m [(m^{\phi} - 1)^2/n^2 + m^{\phi-2} (m^{\phi} - 2)], \\ e_1 &= v_6 q_4 mw (1 - wv^2 m^{\phi-2})/n, & e_2 &= v_6 q_4 vw (m^{\phi} - 1)/n, \\ e_3 &= -vv_6 q_4 ww_1, & e_4 &= v_6 q_4 w_1 m, \\ d_5 &= m(1 - wv^2 m^{\phi-2})/n, \\ d_6 &= vv_5 q_3 [(m^{\phi} - 1)^2/n^2 + m^{2\phi-2}] \\ e_5 &= -w_1 v, & e_6 &= -d_5, \end{aligned}$$

and D denotes the discriminant of the field.

⁶Ibid.

A method analogous to that used in the case of a cubic field is used to prove

LEMMA 1. Every ideal divisor of (p) in $R(\mu)$ whose norm is equal to p or p^2 is one of

$$\begin{aligned} M &= [p, x+\omega, y+\Delta, z+\epsilon], & A &= [p, a+\omega, p\Delta, b+c\Delta+\epsilon], \\ G &= [p, g+\omega, h+\Delta, p\epsilon], & S &= [p, p\omega, j+k\omega+\Delta, s+t\omega+\epsilon]. \end{aligned}$$

7. Factorization of (p) when $(w|p) = -1$. If $x + \omega$ is contained in a factor of (p) , then $(x + \omega)(x - \omega) = x^2 - w$ must be contained in that factor, hence $x^2 - w \equiv 0 \pmod{p}$. But $(w|p) = -1$ and this is impossible. Since $R(\mu)$ is normal, a rational prime factors into a product of conjugate prime ideals in $R(\mu)$; hence, if (p) is not prime, $(p) = SS^*$, S^* conjugate to S . The remaining two conjugate ideals also divide (p) and therefore S must be equal to at least one conjugate. Suppose $S = S'$, that is,

$$\begin{aligned} [p, p\omega, j + k\omega + \Delta, s + t\omega + \epsilon] &= \\ [p, p\omega, j - k\omega + d_5\Delta + d_6\epsilon, s - t\omega + e_5\Delta + e_6\epsilon]. \end{aligned}$$

Then

$$\begin{aligned} j - k\omega + d_5\Delta + d_6\epsilon &= a_1p + a_2p\omega + a_3(j + k\omega + \Delta) \\ &\quad + a_4(s + t\omega + \epsilon), \\ s - t\omega + e_5\Delta + e_6\epsilon &= a_5p + a_6p\omega + a_7(j + k\omega + \Delta) \\ &\quad + a_8(s + t\omega + \epsilon); \end{aligned}$$

hence

$$\begin{aligned} (1) \quad & (d_5 + 1)k + d_6t \equiv 0 \pmod{p}, \\ (2) \quad & (d_5 - 1)j + d_6s \equiv 0 \pmod{p}, \\ (3) \quad & (e_6 + 1)t + e_5k \equiv 0 \pmod{p}, \\ (4) \quad & (e_6 - 1)s + e_5j \equiv 0 \pmod{p}. \end{aligned}$$

Eliminating k between (1) and (3), we find

$t[e_5d_6 - (d_5 + 1)(e_6 + 1)] \equiv 0 \pmod{p}$. Since $e_6 = -d_5$ and $d_5e_6 - d_6e_5 = 1$, $e_5d_6 - (d_5 + 1)(e_6 + 1) = -2$. Also, w is even and $(w|p) = -1$; hence we have $t \equiv 0 \pmod{p}$. Similarly $j \equiv k \equiv s \equiv 0 \pmod{p}$. Suppose $S = S'''$. Since $\omega''' = \omega'$, $\Delta''' = -\Delta'$, $\epsilon''' = -\epsilon'$, we have only to replace d_5, d_6, e_5, e_6 by their negatives in (1), ..., (4). Again $j \equiv k \equiv s \equiv t \equiv 0 \pmod{p}$. Finally, suppose $S = S''$; hence

$$[p, p\omega, j+k\omega+\Delta, s+t\omega+\epsilon] = [p, p\omega, j+k\omega-\Delta, s+t\omega-\epsilon].$$

Therefore

$$j + k\omega - \Delta = a_1p + a_2p\omega + a_3(j + k\omega + \Delta) + a_4(s + t\omega + \epsilon),$$

$$s + t\omega - \epsilon = a_5p + a_6p\omega + a_7(j + k\omega + \Delta) + a_8(s + t\omega + \epsilon),$$

and $j \equiv k \equiv s \equiv t \equiv 0 \pmod{p}$. Consequently S divides S^* , a prime ideal; hence $S = S^*$ and all conjugate ideals are equal. Since (p) is divisible by the square of a prime ideal if and only if $(D|p) = 0$, we have^{*}

THEOREM 1. If $(w|p) = -1$ and $(D|p) = 0$, the prime factorization of (p) in $R(\mu)$ is given by

$$(p) = [p, p\omega, \Delta, \epsilon]^2,$$

but if $(w|p) = (D|p) = -1$, (p) is prime.

8. Factorization of (p) when $(w|p) \neq -1$. Consider first $(w|p) = 1$. In the quadratic⁷ sub-field $R(\omega)$, $(p) = [p, u + \omega][p, u - \omega]$, $u^2 \equiv w \pmod{p}$. Thus in $R(\mu)$, (p) is the product of the conjugate ideals $N = (p, u + \omega)$ and $N' = (p, u + \omega')$ each of norm p^2 . The integer $u + \omega$ cannot be in S , for $u + \omega = a_1p + a_2p\omega + a_3(j + k\omega + \Delta) + a_4(s + t\omega + \epsilon)$ is impossible in integers. Hence, by Lemma 1, $N = A$ or G .

⁷J. Sommer, Vorlesungen über Zahlentheorie, 1907, pp. 61-62.

We compute the closure conditions for G . No conditions are obtained from expressing $p\omega$, $p\Delta$, or $p\epsilon$ in the form

$$\alpha_1 = a_{11}p + a_{21}(g + \omega) + a_{31}(h + \Delta) + a_{41}p\epsilon.$$

The subscript 1 will be considered as taking values from 1 to 8. From $\omega(g + \omega) = w + g\omega = \alpha_4$ and $\epsilon(h + \Delta) = e_1 + e_2\omega + h\epsilon = \alpha_5$ are found

$$(5) \quad g^2 \equiv w \pmod{p}, \quad h \equiv 0 \pmod{p}, \quad e_2g - e_1 \equiv 0 \pmod{p}.$$

The new conditions arising from $\Delta(g + \omega) = (g + d_1)\Delta + d_2\epsilon = \alpha_6$, $\epsilon(g + \omega) = w_1n\Delta + (g - d_1)\epsilon = \alpha_7$, $\Delta(h + \Delta) = d_3 + d_4\omega + h\Delta = \alpha_8$ are

$$(6) \quad d_2 \equiv 0 \pmod{p}, \quad g \equiv d_1 \pmod{p}, \quad d_4g - d_3 \equiv 0 \pmod{p}.$$

No further conditions arise.

If $d_2 \not\equiv 0 \pmod{p}$, both N and N' must be of the form A . Certain of the closure conditions for A are obtained by expressing $\omega(a + \omega) = w + a\omega$, $\Delta(a + \omega) = (a + d_1)\Delta + d_2\epsilon$, and $\Delta(b + c\Delta + \epsilon) = e_1 + cd_3 + (e_2 + cd_4)\omega + b\Delta$ in the form $\beta = b_1p + b_2(a + \omega) + b_3p\Delta + b_4(b + c\Delta + \epsilon)$. We find

$$(7) \quad a^2 \equiv w \pmod{p}, \quad d_2c \equiv d_1 + a \pmod{p},$$

$$(8) \quad b \equiv 0 \pmod{p}.$$

If $d_2 = v_5q_3(1 - wv^2m^{2\phi-2})/n \equiv 0 \pmod{p}$, then $1 - wv^2m^{2\phi-2} \equiv 0 \pmod{p}$, for $w = v_5q_3w_1$ is prime to p . Therefore $w = w^2v^2m^{2\phi-2} \equiv d_1^2 \pmod{p}$. Thus $d_2 \equiv 0 \pmod{p}$ and $g^2 \equiv w \pmod{p}$ imply $g^2 \equiv d_1^2 \pmod{p}$. If $u \equiv -d_1 \pmod{p}$, we may replace u by $-u$ without loss of generality. Thus let $u \equiv d_1 \pmod{p}$. Then it can be shown that $g \equiv u \pmod{p}$, $h \equiv 0 \pmod{p}$ satisfy (5) and (6), hence that $N = G$. If $N' = G$, $-u \equiv -d_1 \equiv g$

$(\text{mod } p)$, a contradiction to (6). Thus $N' = A$, where

$$(9) \quad a \equiv -d_1 \pmod{p}, \quad b \equiv 0 \pmod{p},$$

$$(10) \quad 2d_1c + w_1n \equiv 0 \pmod{p}.$$

Congruence (10) follows from $\epsilon(a + \omega) = b_1p + b_2(a + \omega) + b_3p\Delta + b_4(b + c\Delta + \epsilon)$ and $a \equiv -d_1 \pmod{p}$. Note that $2d_1 \not\equiv 0 \pmod{p}$ since w is even, $(w|p) = 1$, and $w \equiv d_1^2 \pmod{p}$.

LEMMA 2. (a) Let $(w|p) = 1$. If $d_2 \not\equiv 0 \pmod{p}$, a factorization, not necessarily prime, of (p) in $R(\mu)$ is given by

$$(p) = [p, a + \omega, p\Delta, c\Delta + \epsilon][p, a - \omega, p\Delta, c'\Delta + \epsilon],$$

where a and c are determined by (7) and $d_2c' \equiv d_1 - a \pmod{p}$.

$$(b) \quad \text{Let } (w|p) = 1. \text{ If } d_2 \equiv 0 \pmod{p},$$

$$(p) = [p, d_1 + \omega, \Delta, p\epsilon][p, d_1 - \omega, p\Delta, c\Delta + \epsilon],$$

where c is determined by (10).

We consider further factorization of (p) . The closure conditions for M are

$$(11) \quad x^2 \equiv w \pmod{p},$$

$$(12) \quad y(x + d_1) + d_2z \equiv 0 \pmod{p},$$

$$(13) \quad z(x - d_1) + w_1ny \equiv 0 \pmod{p},$$

$$(14) \quad y^2 + d_4x - d_3 \equiv 0 \pmod{p},$$

$$(15) \quad yz + e_2x - e_1 \equiv 0 \pmod{p},$$

$$(16) \quad z^2 + e_4x - e_3 \equiv 0 \pmod{p}.$$

Since $(D|p) = 0$ is necessary and sufficient for (p) to be divisible by the square of a prime ideal, $(D|p) = 0$ implies further factorization. For the two factors in part (a) of Lemma 2 are equal only if $2a \equiv 0 \pmod{p}$, and the two factors in part (b) are equal only if $2d_1 \equiv 0 \pmod{p}$. In either case it is implied

that $w \equiv 0 \pmod{p}$ contrary to the assumption. Moreover, $(w|p) \neq (D|p) = 0$ implies $d_4 \equiv d_3 \equiv e_4 \equiv e_3 \equiv 0 \pmod{p}$; hence

$$(17) \quad (p) = [p, x + \omega, \Delta, \epsilon]^2 [p, x - \omega, \Delta, \epsilon]^2,$$

x determined by (11).

Henceforth assume $(D|p) \neq 0$. If $d_2 \not\equiv 0 \pmod{p}$ and (14) has a solution, determine x by (11), y by (14), and z by (12). Then (13), (15), and (16) hold; hence $(p) = MM'M''M'''$. If $d_2 \equiv 0 \pmod{p}$, take $x \equiv d_1 \pmod{p}$. From (12), $y \equiv 0 \pmod{p}$. If z can be determined by (16), then (11) and (13), (14), and (15) hold. Therefore (p) is a product of four distinct conjugate prime ideals. Theorem 2 can now be verified readily.

THEOREM 2. Let $(w|p) = 1$ and $x^2 \equiv w \pmod{p}$. If $(D|p) = 0$, the prime factorization of (p) in $R(\mu)$ is given by (17). If $(D|p) = 1$, $d_2 \not\equiv 0 \pmod{p}$, and $(d_3 - xd_4|p) = -1$, the prime factorization of (p) is given in Lemma 2, part (a). However, if $(d_3 - xd_4|p) = 1$, (p) is the product of

$$\begin{aligned} [p, x+\omega, y+\Delta, z+\epsilon], & \quad [p, x-\omega, e_6y-d_6z+\Delta, d_5z-e_5y+\epsilon], \\ [p, x+\omega, y-\Delta, z-\epsilon], & \quad [p, x-\omega, d_6z-e_6y+\Delta, e_5y-d_5z+\epsilon], \end{aligned}$$

where y and z are determined by (14) and (12). Finally, if $(D|p) = 1$, $d_2 \equiv 0 \pmod{p}$, and $(e_3 - d_1e_4|p) = -1$, the prime factorization of (p) is given in Lemma 2, part (b), but if $(e_3 - d_1e_4|p) = 1$, (p) is the product of

$$\begin{aligned} [p, d_1+\omega, \Delta, z+\epsilon], & \quad [p, d_1-\omega, d_6z-\Delta, d_5z+\epsilon], \\ [p, d_1+\omega, \Delta, z-\epsilon], & \quad [p, d_1-\omega, d_6z+\Delta, d_5z-\epsilon], \end{aligned}$$

where z is determined by (16).

There remains to consider the case $(w|p) = 0$. In⁸ $R(\omega)$, $(p) = [p, \omega]^2$. Since p divides w , we have $d_1 \equiv d_3 \equiv e_1 \equiv e_3 \equiv 0 \pmod{p}$, hence $x \equiv y \equiv z \equiv 0 \pmod{p}$ satisfy (11), ..., (16).

THEOREM 3. If $(w|p) = 0$, the prime factorization of (p) in $R(\mu)$ is given by

$$(p) = [p, \omega, \Delta, \epsilon]^4.$$

⁸Ibid.

CHAPTER III

CERTAIN NON-CYCLIC QUARTIC FIELDS

In this chapter, a certain type of non-cyclic quartic field is considered. The determination of the prime ideals of these fields is somewhat more complicated than in the type of quartic field previously discussed.

9. Bases of certain non-cyclic quartic fields. Consider a quartic field $R(\lambda')$, where λ' is a root of an equation with rational coefficients whose group with respect to R is the "Vierergruppe." Then $R(\lambda') = R(\lambda)$ where λ satisfies the equation

$$f(z) \equiv z^4 - 2s(r+1)z^2 + s^2(r-1)^2 = 0$$

with s a product of distinct odd primes, r a product of distinct primes, and $r \neq 1$, $s \neq 1$, $r \neq s$. The roots of $f(z) = 0$ are λ , $-\lambda$, $g(\lambda) = s(r-1)/\lambda$, and $-g(\lambda)$. We define the conjugates to $\lambda = \lambda(\lambda)$ as before.

Let $\gamma^2 = r$, $\sigma^2 = s$, and then $R(\gamma)$, $R(\sigma)$ are quadratic subfields of $R(\lambda)$. Define $(r, s) = q$, $q\mu = \gamma\sigma$, $\pi\sigma = \nu$, $2\pi = 1 + \gamma$. If $r \equiv s \equiv 1 \pmod{4}$, a basis⁹ of $R(\lambda)$ is given by

$$1, \pi, \alpha = (1 + \mu)/2, \beta = (\pi + \nu)/2.$$

The following formulae can be verified readily:

⁹A. A. Albert, The integers of normal quartic fields, Annals of Mathematics, vol. 31 (1930), pp. 381-418.

$$\begin{aligned}
\lambda^2 &= s(r-1) + 4s\pi, & [g(\lambda)]^2 &= s(r+3-4\pi), \\
g(\lambda) &= -2q + 2\pi + 4q\alpha - 4\beta, \\
\sigma &= [\lambda^3 - s(r+3)\lambda]/2s(r-1), \\
\pi\alpha &= a_1 + a_2\pi - 2a_1\alpha + a_3\beta, & \pi^2 &= a_1 + \pi, \\
\pi\beta &= b_1 - a_1\pi - qa_1\alpha + b_2\beta, & \alpha^2 &= b_3 + \alpha, \\
\alpha\beta &= e_1 + e_2\pi - a_1\alpha + e_3\beta, & \beta' &= f_1 + q\alpha - \beta, \\
\beta^2 &= e_4 + qe_2\pi - qa_1\alpha + b_2\beta, & \beta'' &= \pi - \beta, \\
\sigma' &= -q + 2\pi + 2q\alpha - 4\beta, & \beta''' &= f_2 - \pi - q\alpha + \beta, \\
1 - \pi &= 1 - \pi'' = \pi' = \pi''', & D &= r^2s^2/q^2, \\
1 - \alpha &= 1 - \alpha' = \alpha'' = \alpha''',
\end{aligned}$$

where

$$\begin{aligned}
a_1 &= (r-1)/4, & a_2 &= (q-r)/2q, & a_3 &= r/q, \\
b_1 &= a_1(q+1)/2, & b_2 &= (r+1)/2, & b_3 &= (rs-q^2)/4q^2, \\
e_1 &= a_1(q+s)/2q, & e_2 &= (s-r)/4q, & e_3 &= (r+q)/2q, \\
e_4 &= a_1(1+s+2q)/4, & f_1 &= (1-q)/2, & f_2 &= (1+q)/2,
\end{aligned}$$

and D denotes the discriminant of the field.

10. Factorization of (p) when $(4r|p) = -1$. As in the previous cases, we have

LEMMA 1. Every ideal divisor of (p) in $R(\lambda)$ whose norm is equal to p or p^2 is one of

$$\begin{aligned}
L &= [p, x+\pi, y+\alpha, z+\beta], & F &= [p, c+\pi, p\alpha, f+g\alpha+\beta], \\
E &= [p, e+\pi, h+\alpha, p\beta], & U &= [p, p\pi, u+v\pi+\alpha, m+n\pi+\beta].
\end{aligned}$$

Suppose an ideal factor not the unit ideal of $(p) \neq (2)$ contains an integer $x + \pi$. Then $4(x + \pi)(x + \pi') = 4(x^2 + x - a_1) \equiv 0 \pmod{p}$; hence $(r|p) = 1$ or 0 . Thus if $(4r|p) = -1$, any factor of (p) must be of the form U . Since $R(\lambda)$ is normal, (p) is a product of two conjugate ideals. Let $(p) = UU'$, where

$$U' = [p, p\pi, u + v(1 - \pi) + \alpha, m + n(1 - \pi) + f_1 + q\alpha - \beta].$$

Therefore the coefficients of $1, \pi, \alpha, \beta$ in

$$\begin{aligned} (u + v\pi + \alpha)(u + v - v\pi + \alpha) &= (u^2 + uv - a_1v^2 + b_3) + x_1\pi \\ &\quad + (2u + v + 1)\alpha + x_2\beta, \\ (u + v\pi + \alpha)(m + n + f_1 - n\pi + q\alpha - \beta) &= \\ &\quad x_3 + x_4\pi + x_5\alpha + [v(a_3q - b_2) - u - na_3 - e_3]\beta, \\ (m + n\pi + \beta)(m + n + f_1 - n\pi + q\alpha - \beta) &= \\ &\quad x_6 + x_7\pi + mq\alpha + x_8\beta, \end{aligned}$$

must be divisible by p . The x_i are certain rational integers that can be computed readily. Since $a_3q - b_2 = 2a_1$ and $(q, p) = 1$, we have

$$(1) \quad m \equiv 0 \pmod{p}, \quad a_3n \equiv 2a_1v - u - e_3 \pmod{p}.$$

Eliminating v between $u^2 + uv - a_1v^2 + b_3 \equiv 0 \pmod{p}$ and

$$(2) \quad v + 2u + 1 \equiv 0 \pmod{p},$$

we have

$$(3) \quad qu^2 + qu + (q^2 - s)/4q \equiv 0 \pmod{p}.$$

Let $(p) = UU'''$, where

$$U''' = [p, p\pi, u+v(1-\pi)+(1-\alpha), m+n(1-\pi)+f_2-\pi-q\alpha+\beta].$$

Then the coefficients of $1, \pi, \alpha, \beta$ in

$$\begin{aligned} (u + v\pi + \alpha)(u + v + 1 - v\pi - \alpha) &= \\ &\quad (u^2 + uv - a_1v^2 - 2a_1v + u - b_3) + y_1\pi + rv\alpha + y_2\beta, \\ (m + n\pi + \beta)(u + v + 1 - v\pi - \alpha) &= y_3 + y_4\pi \\ &\quad + (qa_1v + 2a_1n - m + a_1)\alpha + [u - a_3n + (1 - b_2)v + 1 - e_3]\beta, \end{aligned}$$

must be divisible by p . The y_i are certain rational integers. Since $(r, p) = 1$, $v \equiv 0 \pmod{p}$ and the following congruences

must hold:

$$(4) \quad v \equiv 0 \pmod{p}, \quad a_3 n \equiv u + a_2 \pmod{p}, \quad m \equiv a_1(2n + 1) \pmod{p},$$

$$(5) \quad u^2 + u - b_3 \equiv 0 \pmod{p}.$$

Congruence (3) has a solution if and only if $(s|p) \neq -1$, while congruence (5) has a solution if and only if $(rs/q^2|p) \neq -1$. Moreover, if $(rs/q^2|p) = -1$, $(r^2s/q^2|p) = +1$ and $(s|p) = +1$.

The closure conditions for U are given by

$$(6) \quad \begin{aligned} n(b_2 + nb_2 + m) - qa_1(1 + n)v + a_1n - qe_2 &\equiv 0 \pmod{p}, \\ m(b_2 + nb_2 + m) - qa_1(1 + n)u - b_1n - e_4 &\equiv 0 \pmod{p}, \\ u(-a_1 - 2a_1n + m) + m(e_3 + a_3n) - a_1n - e_1 &\equiv 0 \pmod{p}, \\ m(e_3 + b_2v + u) - a_1(1 + qv)u - b_1v - e_1 &\equiv 0 \pmod{p}, \\ v(-a_1 - 2a_1n + m) + n(e_3 - a_2 + a_3n) - e_2 &\equiv 0 \pmod{p}, \\ u(1 - 2a_1v + u) + v(-a_1 + a_3m) - b_3 &\equiv 0 \pmod{p}, \\ n(e_3 + b_2v + u) - qa_1v^2 - e_2 &\equiv 0 \pmod{p}, \\ m + n(1 - b_2) + qa_1v - a_1 &\equiv 0 \pmod{p}, \\ v(1 - a_2 + a_3n - 2a_1v + u) &\equiv 0 \pmod{p}, \\ b_2m - a_1(n + qu) - b_1 &\equiv 0 \pmod{p}, \\ u + (2a_1 + 1)v + a_2 - na_3 &\equiv 0 \pmod{p}, \\ a_1(2u + v + 1) - ma_3 &\equiv 0 \pmod{p}. \end{aligned}$$

If $(rs/q^2|p) = 1$, determine u by (5) and v, n, m by (4). It can be shown that (6) is satisfied. Since $(D|p) \neq 0$, the remaining conjugate factor is distinct from $U = U'$ and $(p) = UU''$. If $(rs/q^2|p) = -1$, determine u by (3), v by (2), and m, n by (1). Then (6) is satisfied. In this case $U = U'''$ and $(p) = UU''$.

Finally, let $(rs/q^2|p) = 0$; hence $(D|p) = 0$ and all conjugate ideals are equal. We therefore take $v = m = 0$,

$$(7) \quad 2u + 1 \equiv 0 \pmod{p}, \quad 2n + 1 \equiv 0 \pmod{p}.$$

THEOREM 1. Let $(4r|p) = -1$. If $(rs/q^2|p) = 1$, the prime factors of (p) in $R(\lambda)$ are

$$[p, p\pi, u + \alpha, m + n\pi + \beta],$$

$$[p, p\pi, u + 1 - \alpha, m + (n + 1)\pi - \beta],$$

where u, n, m are determined by (5) and (4). If $(rs/q^2|p) = -1$, the required factors are

$$[p, p\pi, u + v\pi + \alpha, n\pi + \beta],$$

$$[p, p\pi, u + 1 + v\pi - \alpha, (n + 1)\pi - \beta],$$

where u, v, n are determined by (3), (2), and (1). If $(rs/q^2|p) = 0$, then the required factorization is

$$(p) = [p, p\pi, u + \alpha, n\pi + \beta]^2,$$

where u and n are determined in (7).

11. Factorization of (p) when $(4r|p) = 1$. In the quadratic sub-field¹⁰ $R(\chi)$, $(p) = [p, a + \pi][p, a + \pi']$, where $(2a + 1)^2 \equiv r \pmod{p}$; hence in $R(\lambda)$, (p) is a product of two conjugate ideals of norm p^2 . Since $a + \pi$ is not in U , $(p, a + \pi)$ must equal E or F . The condition $\alpha(e + \pi) = a_1 + a_2\pi + (e - 2a_1)\alpha + a_3\beta = z_1p + z_2(e + \pi) + z_3(h + \alpha) + z_4p\beta$, the z_1 rational integers, requires $a_3 \equiv 0 \pmod{p}$, contrary to the assumption. Thus both conjugate ideals are of the form F . Since $a + \pi$ is in F , $c \equiv a \pmod{p}$. The condition $\alpha(a + \pi) = a_1 + a_2\pi + (a - 2a_1)\alpha + a_3\beta = z_5p + z_6(a + \pi) + z_7p\alpha + z_8(f + g\alpha + \beta)$ gives a unique determination for f and g :

$$(8) \quad a_3f \equiv a_1 - aa_2 \pmod{p}, \quad a_3g \equiv a - 2a_1 \pmod{p}.$$

¹⁰J. Sommer, Vorlesungen über Zahlentheorie, 1907, pp. 62-63.

LEMMA 2. If $(4r|p) = 1$, a factorization of (p) in $R(\lambda)$ is given by

$$(p) = [p, a + \pi, p\alpha, f + g\alpha + \beta][p, a + 1 - \pi, p\alpha, f + f_1 + (g + q)\alpha - \beta]$$

where $(2a + 1)^2 \equiv 0 \pmod{p}$ and f, g are determined in (8).

We consider further factorization of F and F' . The closure conditions for L are

$$(9) \quad z^2 + b_2z - qa_1y + qe_2x - e_4 \equiv 0 \pmod{p},$$

$$(10) \quad y(z - a_1) + e_3z + e_2x - e_1 \equiv 0 \pmod{p},$$

$$(11) \quad z(x + b_2) - qa_1y - a_1x - b_1 \equiv 0 \pmod{p},$$

$$(12) \quad y(x - 2a_1) + a_3z + a_2x - a_1 \equiv 0 \pmod{p},$$

$$(13) \quad x^2 + x - a_1 \equiv 0 \pmod{p},$$

$$(14) \quad y^2 + y - b_3 \equiv 0 \pmod{p}.$$

If $(rs/q^2|p) = -1$, (14) has no solution, L does not exist, and F, F' are prime. Suppose (14) does have a solution y . Then x determined by (13) and z by (12) satisfy (9), (10), and (11) and $(p) = LL'L''L'''$.

THEOREM 2. Let $(4r|p) = 1$. If $(rs/q^2|p) = -1$, the prime factorization of (p) in $R(\lambda)$ is given in Lemma 2, but if $(rs/q^2|p) \neq -1$, (p) is the product of

$$[p, x + \pi, y + \alpha, z + \beta],$$

$$[p, x + 1 - \pi, y + \alpha, qy - z - f_1 + \beta],$$

$$[p, x + \pi, y + 1 - \alpha, x - z + \beta],$$

$$[p, x + 1 - \pi, y + 1 - \alpha, z + f_2 - x - 1 - qy - q + \beta],$$

where x, y , and z are determined by (13), (14), and (12).

Note that $(rs/q^2|p) = 0$ implies (p) divisible by the square of a prime ideal.

12. Factorization of (p) when $(r|p) = 0$. In this case,¹¹
 $(p) = (p, p_1 + \pi)^2$, where $p_1 = (p - 1)/2$, and $(p, p_1 + \pi)$
 equals E or F .

If p divides q , $a_3 \not\equiv 0 \pmod{p}$ and E does not exist, for
 $\alpha(e + \pi) = z_1 p + z_2(e + \pi) + z_3(h + \alpha) + z_4 p^\beta$ implies
 $a_3 \equiv 0 \pmod{p}$. Then

$$(15) \quad (p) = [p, p_1 + \pi, p\alpha, f + g\alpha + \beta]^2,$$

where f and g are determined by (8) with $a \equiv p_1 \pmod{p}$. Since
 $q \equiv 0 \pmod{p}$, these congruences are equivalent to

$$(16) \quad 4f + 1 \equiv 0 \pmod{p}, \quad g \equiv 0 \pmod{p}.$$

Moreover, (14) is equivalent to

$$(17) \quad (2y + 1)^2 \equiv rs/q^2 \pmod{p};$$

hence $(rs/q^2|p) = -1$ implies that the above factorization is
 prime. If $(rs/q^2|p) = 1$, (17) has a solution y and if z is de-
 termined by

$$(18) \quad 4z + 1 \equiv 0 \pmod{p},$$

(9), ..., (14) hold and F factors further.

The closure conditions for E are given by

$$(19) \quad \begin{aligned} h(e - 2a_1) - a_1 + a_2 e &\equiv 0 \pmod{p}, \\ a_1 e + qa_1 h + b_1 &\equiv 0 \pmod{p}, \\ e_2 e - a_1 h - e_1 &\equiv 0 \pmod{p}, \\ h^2 + h - b_3 &\equiv 0 \pmod{p}, \\ e^2 + e - a_1 &\equiv 0 \pmod{p}, \\ e + b_2 &\equiv 0 \pmod{p}, \\ h + e_3 &\equiv 0 \pmod{p}, \\ a_3 &\equiv 0 \pmod{p}. \end{aligned}$$

¹¹Ibid.

If p divides a_3 , take $e = h = p_1$. Then the closure conditions (19) are satisfied and

$$(20) \quad (p) = [p, p_1 + \pi, p_1 + \alpha, p\beta]^2.$$

Since p divides a_3 , (14) becomes

$$(21) \quad 2y + 1 \equiv 0 \pmod{p},$$

and (9) with $x = p_1$ and $2y \equiv -1 \pmod{p}$ becomes

$$(22) \quad (4z + 1)^2 \equiv s \pmod{p}.$$

Hence if $(s|p) = -1$, the above factorization is prime. If $(s|p) = 1$, the closure conditions (9), ..., (14) can be satisfied and E factors further. The following theorem can now be established readily.

THEOREM 3. Let $(q|p) = 0$. If $(rs/q^2|p) = -1$, the prime factorization of (p) in $R(\lambda)$ is given in (15) with f and g determined by (16). If $(rs/q^2|p) = 1$, then

$$(p) = [p, p_1 + \pi, y + \alpha, z + \beta]^2 [p, p_1 + \pi, y + 1 - \alpha, z + \beta]^2$$

where y is determined by (17) and z by (18). Next, let $(a_3|p) = 0$. If $(s|p) = -1$, the prime factorization of (p) is given in (20), but if $(s|p) = 1$, we have

$$(p) = [p, p_1 + \pi, p_1 + \alpha, z + \beta]^2 [p, p_1 + \pi, p_1 + \alpha, p_1 - z + \beta]^2,$$

where z is determined by (22).

13. The prime factors of (2). Suppose $(r|2) = -1$, that is, $r \equiv 5 \pmod{8}$. Then no factor of (2) can contain an integer $x + \pi$, for $4(x + \pi')(x + \pi) = (2x + 1)^2 - r \equiv 0 \pmod{8}$ is impossible. Thus if (2) has a factor, it must be of the form U .

Let $s \equiv 5 \pmod{8}$ and choose $v + 1 \equiv m \equiv 1 \pmod{2}$, $u \equiv n + 1 + e_3 \pmod{2}$. Then (6) holds and the factors of (2) are

$$(23) \quad [2, 2\pi, e_3 + \alpha, 1 + \pi + \beta], \quad [2, 2\pi, e_3 + 1 + \alpha, 1 + \beta].$$

Let $s \equiv 1 \pmod{8}$ and choose $v \equiv m + 1 \equiv 1 \pmod{2}$, $u \equiv n + e_3 \pmod{2}$. As before, the factors of (2) are

$$(24) \quad [2, 2\pi, e_3 + \pi + \alpha, \beta], \quad [2, 2\pi, e_3 + 1 + \pi + \alpha, \pi + \beta].$$

If $(r|2) = 1$, or $r \equiv 1 \pmod{8}$, $(2) = (2, \pi)(2, \pi')$.¹² These factors are prime if $s \equiv 5 \pmod{8}$, for then (14) has no solution. We determine their bases in $R(\lambda)$. Since π is not in U and $(2, \pi)$, $(2, \pi')$ have norm 2^2 , they are either of the form E or F . But $\alpha(e + \pi)$ in E demands a_3 even, contrary to the assumption. Therefore each factor is of the form F and c of F is even. By writing $\alpha\pi = a_1 + a_2\pi - 2a_1\alpha + a_3\beta = 2z_1 + z_2\pi + 2z_3\alpha + z_4(f + g\alpha + \beta)$, we see that (2) has the factors

$$(25) \quad [2, \pi, 2\alpha, \beta], \quad [2, 1 + \pi, 2\alpha, f_1 + \alpha + \beta].$$

If (14) has a solution, or in other words if $s \equiv 1 \pmod{8}$, we may take x even or odd, y even or odd, and $z \equiv x(a_2 + y) \pmod{2}$. Then (9), ..., (14) are satisfied and the prime factors of (2) are

$$(26) \quad [2, \pi, \alpha, \beta], \quad [2, 1 + \pi, \alpha, a_2 + \beta], \\ [2, \pi, 1 + \alpha, \beta], \quad [2, 1 + \pi, 1 + \alpha, a_2 + 1 + \beta].$$

THEOREM 4. When $(r|2) = -1$, the prime factors of (2) in $R(\lambda)$ are given by (23) or (24), according as $(s|2) = -1$ or $+1$. If $(r|2) = 1$, the prime factors of (2) are given in (25) or (26) according as $(s|2) = -1$ or $+1$.

¹²Ibid.

VITA

Harriet Rees was born at Mt. Morris, Illinois, in 1914. She received her elementary and high school education in the public schools at Mt. Morris. During the years 1930-1934 she attended Rockford College, and received the degree of Bachelor of Arts from there in 1934. She began her graduate work at the University of Chicago in October of that year, and was granted an M.S. degree in August, 1935. She continued her study at the University until June, 1937. She wishes to express her gratitude to the professors under whom she studied, Professors Albert, Barnard, Bartky, Bliss, Dickson, Graves, Lane, Logsdon, MacMillan, and Reid. In particular, she wishes to express to Professor Albert her appreciation of his assistance during the preparation of this dissertation.

